

BUILDING A BASIS FOR INFORMATION WARFARE RULES OF ENGAGEMENT

**A MONOGRAPH
BY
Major Ted T. Uchida
United States Air Force**



**School of Advanced Military Studies
United States Army Command and General Staff
College
Fort Leavenworth, Kansas**

First Term AY 97-98

Approved for Public Release Distribution is Unlimited

DTIC QUALITY INSPECTED 3

19980324 099

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 18 December 1997		3. REPORT TYPE AND DATES COVERED MONOGRAPH
4. TITLE AND SUBTITLE <i>BUILDING A BASIS FOR INFORMATION WARFARE RULES OF ENGAGEMENT</i>			5. FUNDING NUMBERS	
6. AUTHOR(S) <i>MAJ TED T. UCHIDA, USAF</i>				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SCHOOL OF ADVANCED MILITARY STUDIES COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH, KANSAS 66027			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH, KANSAS 66027			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT DISTRIBUTION UNLIMITED			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) SEE ATTACHED				
14. SUBJECT TERMS			15. NUMBER OF PAGES <i>WP 65</i>	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED		18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED		19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED
				20. LIMITATION OF ABSTRACT UNLIMITED

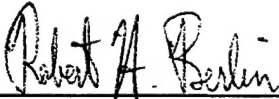
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Ted T. Uchida

Title of Monograph: *Building a Basis for Information Warfare Rules of Engagement*

Approved by:



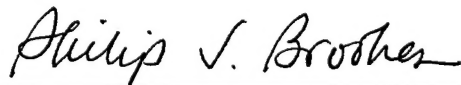
Robert H. Berlin, Ph.D.

Monograph Director



COL Danny M. Davis, MA, MMAS

Director, School of Advanced
Military Studies



Philip J. Brookes, Ph.D.

Director, Graduate Degree
Program

Accepted this 18th Day of December 1997

DTIC QUALITY INSPECTED 3

ABSTRACT

BUILDING A BASIS FOR INFORMATION WARFARE RULES OF ENGAGEMENT by Major Ted T. Uchida, USAF, 62 pages.

The US armed forces face a global information threat which could launch an attack without warning. This surprise attack could damage the US armed forces ability to mobilize, deploy and control forces worldwide. The attack will use the global information infrastructure to target the information-based processes the US armed forces utilize to dominate the entire spectrum of conflict. To protect information based processes, US armed forces joint operational planners are building plans to defeat and possibly attack information-based threats. This monograph discusses how the US armed forces should regulate the defensive and offensive responses to information attack with Rules of Engagement.

After defining several terms, this monograph illustrates the gravity of the threat the US armed forces face in the information spectrum. The proliferation of computers and networking is creating a huge underclass of IW warriors bent on destroying, manipulating, and stealing information. While past IW threats were curious "hackers," the modern IW environment is encompassed by over 18 countries currently pursuing active IW attack and defense programs. Dealing with a threat requires operational planners recognize that information is rapidly becoming the center of gravity for military operations. This monograph proposes IW planners build IW ROE that extends maximum protection to information by protecting key information systems and infrastructure. Additionally, IW ROE should also allow the US armed forces to autonomously implement retaliatory or pre-emptive self defensive actions to counter any information based threat.

After describing the areas IW ROE should carefully consider, the monograph examines the inadequacies of purely defensive IW policies, centrally controlled IW attack response, and the legal, historical, and theoretical justification for retaliatory and pre-emptive IW ROE. This monograph concludes by recommending the US develop a national information policy, military information strategy, and single DoD focal point for IW. A national information policy outlines legal, political, and moral constraints for military operations. A military information strategy translates national policies into concrete objectives for operational planners to build upon. Finally, a single focal point for IW affairs facilitates cohesive IW attack and defense plans by combining all IW affairs under one agency.

TABLE OF CONTENTS

CHAPTER 1: THE INFORMATION THREAT.....	1
INTRODUCTION.....	1
CASE STUDY.....	2
DEFINITIONS.....	4
COMPUTER PROLIFERATION AND MILITARY RELIANCE ON COMPUTERS	6
GROWING ATTACKS, VULNERABILITIES, & THREATS	8
SUMMARY.....	11
CHAPTER TWO: CURRENT STATE OF IW AFFAIRS	13
FOUNDATIONAL IW CONCEPTS	13
CURRENT IW DOCTRINE.....	16
LAW OF WAR, ROE & SROE, AND SELF DEFENSE	19
CHAPTER 3: FOUNDATIONAL IW ROE CONCEPTS.....	22
FRAMEWORK FOR PROTECTING IW ROE	22
BUILDING A CASE FOR SELF DEFENSE: THE INADEQUACY OF DEFENSE ALONE	29
BUILDING A CASE FOR SELF DEFENSE: THE INADEQUACY OF CENTRALLY CONTROLLED ATTACK.....	30
SUMMARY.....	32
CHAPTER 4: JUSTIFYING SELF-DEFENSE.....	34
LEGAL JUSTIFICATION FOR SELF-DEFENSE	34
HISTORICAL JUSTIFICATION FOR SELF-DEFENSE.....	36
THEORETICAL JUSTIFICATION FOR SELF-DEFENSE	38
CONCLUSION	42
ENDNOTES	47
BIBLIOGRAPHY.....	57

Chapter 1: The Information Threat

Introduction

The rapid growth of computer based information processing and its application to military operations presents combatants with a new form of warfare. In its defensive manifestations, this new form of warfare aims to protect the US armed forces' ability to electronically acquire, process, and distribute information during military operations spanning the entire spectrum of conflict. Conversely, in its offensive manifestations, this new form of warfare implements actions that prevent adversaries from effectively utilizing information in their operations. The US armed forces call this new form of conflict Information Warfare (IW).

As with any form of warfare, political and military leaders seek to regulate the use of force. IW is no exception. Regulating IW requires that military leaders develop Rules of Engagement (ROE) adhering to the wishes of the US armed forces political leaders and the US interpretation of generally accepted international agreements.¹ However, many problems face those undertaking this task. Balancing the necessity to protect critical information systems from attack against the necessity for barrier free access to information blurs the lines between just and unjust retaliatory and pre-emptive self defensive actions.² The US armed forces doctrinal imperative to centrally control combat operations, balanced against the requirement to execute decentralized operations aggressively and with initiative further complicates the task of formulating IW ROE.³ Assuring rationality predominates during times of extreme uncertainty and chaos in the wartime environment

versus the need to foster an environment of innovation to solve complex problems further complicates the matter of drafting IW ROE. Finally, delineating which critical information processing capabilities to protect requires IW ROE developers study information's critical role during operations and the extent to which US armed forces can justify utilizing self defense for those systems.

To effectively draft IW ROE that balances legal, political, moral and military requirements requires identifying foundational concepts IW ROE developers can utilize to protect information systems, information-based processes, and information infrastructure from IW attack. Outlining these foundational concepts requires an understanding of the IW threat and the vulnerabilities it presents to the US armed forces information-based processing mechanisms. It also requires understanding the purpose for ROE, the current direction of joint IW concepts and doctrine and their link to ROE, and the legal, theoretical, and historical justifications for retaliatory and pre-emptive self defense.

Case Study

The ease with which IW was waged and the damage it caused is illustrated by examining the events surrounding an unauthorized intrusion of Lawrence Berkeley Laboratories (LBL) information system in 1989. The case, dubbed "The Cuckoo's Egg," involved LBL astrophysicist and systems administrator Clifford Stoll's efforts to track and apprehend the intruder and stop him from stealing sensitive government information.⁴

Stoll discovered the presence of an intruder into the LBL computer system by noticing and tracing a minor accounting error. Stoll later realized that he had stumbled upon a critical mistake committed by the intruder. Utilizing his system administrator

computer privileges, Stoll traced the source of the error to an unauthorized network user. He also discovered the intruder had left a program he deemed a "cuckoo's egg."⁵

Utilizing numerous tracing methods, such as hardware and software subroutines that monitored keystrokes sent from the intruder's computer, Stoll discovered the intruder was using the LBL system as a conduit to access systems on Tymnet and other interconnected systems around the nation.⁶ In his struggles to protect the LBL system while watching the intruder, Stoll discovered the intruder's intent was to steal classified information on key US government and Department of Defense projects. Realizing the severity of the situation, Stoll contacted the FBI, NSA, and CIA for help. After getting past paralyzing internal jurisdictional arguments amongst all three agencies, Stoll finally received the help he needed to stop the intruder. Unable to keep the intruder on line long enough to trace him to his source, Stoll devised a sting nicknamed "Operation Showerhead."⁷ The sting utilized bogus information pertaining to the Strategic Defense Initiative (SDI) or "Starwars" program. After seeing the SDI information, the intruder fell for the operation, and remained on line long enough for Stoll to trace him to Hanover, West Germany. Examining the intruder's actions revealed a pattern of international espionage bent on selling classified US Government documents to the KGB.⁸

While the case represents a fascinating look in to one man's effort to track down and apprehend an unauthorized user, several critical vulnerabilities identified by Stoll still exist today. While Stoll faced a network limited primarily to interconnected mainframe computers located in major computer centers, millions of computers and vast networks connecting them together dominate today's environment of computing. Today, intruders, utilizing thousands of entry nodes, can access a globally networked society to plant

viruses, corrupt information systems, and steal classified information. Furthermore, the US armed forces inextricable interconnection with the global network puts at risk many of the same defense information systems entered during the 1989 incident. Additionally, the interagency bureaucracy Stoll faced exists in today's plans to combat IW. An "Aviation Week & Space Technology" article by David Fulghum demonstrated the inability of national intelligence organizations, such as the CIA and NSA to cooperate with the Department of Defense (DoD) on IW employment. Under current plans, the DoD would have to seek permission before employing IW. Interagency coordination looms as a major stumbling block to combating information attacks and employing IW.⁹

Definitions

The language and terminology of IW represents a sea of new ideas and definitions. To establish a baseline of understanding and lend clarity to future discussion requires investigating several key terms. The first term is cyberspace. Cyberspace is the intangible and ethereal medium through which the majority of the electronic and digital information flows. It represents the momentary space between two modes of electronic communications where information resides while it is transiting between sender and receiver. Examples of cyberspace include the airwaves transmitting microwave and cellular signals or information transiting down millions of miles of copper or glass fibers. In common terms, it is where electronic mail or the phone calls reside during transmission or where much of our real and tangible money and wealth, excluding cash in hand, exists.¹⁰

Because of its various definitions and meanings, examining the context and definition of IW also clarifies future discussions. While many differing definitions for IW exist, they all generally include offensive or defensive actions taken to affect enemy information use during strategic, operational, and tactical operations, while preserving friendly use by enabling the free flow of information. In its offensive form, IW seeks to dominate the information spectrum by utilizing minimum force to destroy, corrupt or incapacitate the enemy's ability to acquire, process and distribute information. IW's primary target is information-based decision making functions, not the information technology itself. In its defensive form, IW ensures the free flow of information to US armed forces by constructing barriers, warning indicators, and backup systems.¹¹

Information systems are generally the objective of most IW attacks. An information system is an all inclusive automated or manual system of components, infrastructure, and personnel, organized with specific guidelines and procedures, designed to collect, process, evaluate, store, and disseminate information. Modern information systems can exist discretely as stand alone systems or in networked environments. When networked, information systems generally electronically link together via telephone, microwave, or satellite communications. An example of a military information system is Department of Defense Intelligence Information System (DODIIS). DODIIS is a worldwide computer network of forty nodes utilized to collect, process, store and disseminate electronic, photo, and human intelligence.¹²

The connecting wires, satellites, microwave relays, and other electronic communication mediums represent the information infrastructure connecting information systems together. The information infrastructure includes the direct and indirect paths of

digital connectivity of information systems and computers that allows instantaneous voice, data, and video transmission. Analogous to the interconnecting tissue and skeletal structure of the human body, information infrastructure represents the architecture and framework linking information systems. Inextricably interconnected within the global information infrastructure is the National Information Infrastructure (NII) and Defense Information Infrastructures (DII).¹³

A final term requiring definition is information superiority. Information superiority is the dominating ability of information warfare to control information systems and ensure uninterrupted flow of information. Like air superiority, it can be local or general and does not connote full control over the entire information spectrum.¹⁴

Computer Proliferation and Military Reliance on Computers

Computer proliferation and the growth of interconnectivity in society are astounding. As many as three billion computers currently exist worldwide, with experts predicting continued exponential growth until the year 2005 and continued doubling of microprocessor performance every 18 months.¹⁵ Approximately twenty million people access the Internet, a global network of computers, with projections for approximately one hundred million by the year 2,000. The White House, on average, receives approximately 5,000 E-mail messages weekly while "Time Magazine's" interactive Internet efforts generated two million visits in the first eight months of its operation.¹⁶

Computers and information systems touch every aspect of today's society and control many aspects of everyday life. Placing simple telephone calls rests on the ability of local telephones to connect with a vast network supercomputer controlled electronic

switching and relay stations.¹⁷ Similarly, the interconnection of financial systems represents a networked economy where information about money versus money itself moves.¹⁸ The global interconnection of computers allows equities traders in New York to conduct real-time trades around the clock in global markets such as Hong Kong, Tokyo, London and Paris. However, the global inter-connectivity of financial markets also increases market volatility by transferring market reactions in a country or region globally. For example, a sharp drop in Hong Kong equities markets can result in a frenetic selling spree in London, Paris, and New York.¹⁹ Therefore, information infrastructures and information systems enable a person to make a phone call, a broker to sell a stock, or a businessman to send electronic mail.

At the heart of US national security lays information infrastructure. Vast networks of information systems control key financial, telecommunications, and other infrastructures. For example, the ability for electric utility companies to transfer electricity between internally owned power grids or between grids of neighboring companies relies on networks of nationally connected information systems. Realizing the extreme importance of information systems and information infrastructure to national security, President William J. Clinton, in July of 1996, chartered the President's Commission on Critical Infrastructure Protection (PCCIP) to study vulnerabilities of key infrastructure. The key infrastructure areas identified for study are Information and Communications, Electrical Power Systems, Gas and Oil Transportation and Storage, Banking and Finance, Transportation, Water Supply Systems, Emergency Services, and Government Services. Globally connected information systems represent the common thread linking each of these key infrastructures together.²⁰

The proliferation of, and dependence on information systems and infrastructure also permeates the US armed forces. Over 2.1 million computers, 10,000 local area networks, and 100 long distance networks represents part of the vast DII.²¹

Revolutionary expansion of information systems within the US armed forces continues fueling drives to computerize military data access, accumulation, and dissemination processes. Areas where US armed forces utilize information systems include command and control, administration, communication, research and development, modeling and simulation, and intelligence and targeting. The list of new information systems and information infrastructure is endless. Some examples include the Army's All Source Analysis System (ASAS), the Air Force's Contingency Theater Automated Planning System (CTAPS) and the Navy's Copernicus information infrastructure. Examples of joint information systems include the Defense Switch Network (DSN), Global Command and Control System (GCCS) and Joint Maritime Command Information System (JMCIS).²² While the list is voluminous, it serves to illustrate one salient factor. As the US armed forces increase reliance on information systems and infrastructure, the opportunities to attack the US armed forces information-based processes also grows. Automating and connecting new processes to the DII increases the threat from intruders seeking to steal or corrupt information.

Growing Attacks, Vulnerabilities, & Threats

The rapid growth of the GII, NII, and DII is also facilitating rapid growth of covert and overt IW attacks. The extent of IW attacks on Defense information systems is astounding. The GAO reported that the Defense Information Systems Agency (DISA)

recorded 53 attacks in 1992, 115 attacks in 1993, 255 attacks in 1994 and 559 attacks in 1995 against US military and Department of Defense systems. Furthermore, they expect the number to increase to 14,000 by the year 1999. DISA estimates computer users detected only one in 150 attacks and that the actual number of attacks could be as high as 250,000 annually. Finally, DISA reported a 65% success rate during system security tests and that 98% of both real and test penetrations went undetected.²³

In one case, IW attackers caused considerable damage to US armed forces information systems. The case clearly shows the vulnerability of military information systems and the price paid for poor IW security. Intruders attacked the US Air Force's Rome Laboratories information system. Utilizing the Internet, intruders invaded Rome Labs information system, seized control over it for several days and copied and downloaded critical information. The intrusion went undetected for three days. While the intruders did not inflict any lasting damage on the information system, investigators do not know the status of the stolen information. The Air Force estimated the cost of the attack was approximately \$500,000 in man hours spent on turning off systems, verifying system integrity, installing security patches and restoring service.²⁴ Other high profile attacks against US armed forces information systems included penetration of the US Naval Academy's computer system, penetration by Dutch intruders into 34 Defense sites between April 1990 and May 1991 and penetration of Army Missile Research Laboratory facilities located at White Sands Missile Range.²⁵

Analyzing IW attacks reveals many of the vulnerabilities existing in today's information systems and information infrastructure relate to human factors, drives toward open architecture and interconnection of civilian and military networks. Human factors

contribute to a large majority of the vulnerabilities. Poor password protection, physical security, and lack of vigilance by system administrators allow IW attackers to install “back doors” and steal, alter, and destroy critical information.²⁶ Drives toward designing open network architecture increases the vulnerability of intruders attacking the information system. Protocol-based weaknesses in authentication and cryptosystem weaknesses involving inadequate key size demonstrate further information system vulnerabilities.²⁷ Finally, heavy use of civilian phone switching equipment by the US armed forces makes DII vulnerable to indirect IW attack from adversaries utilizing civilian phone switching connections.

While the demonstrated vulnerabilities are serious, the potential harm from coordinated physical and IW attack poses an additional threat to US armed forces. IW attack could be used synergistically in a theater campaign as the blinding mechanism preceding an all out conventional attack. Rendering key command and control systems

Top Ten Information Warfare Targets

1. *Culpeper (Virginia) electronic switch which handle all Federal funds and transactions.*
2. *Alaska pipeline which carries 10 percent of all US domestic oil.*
3. *Electronic switching system which manages all telephony.*
4. *Internet.*
5. *Time distribution system*
6. *Panama Canal.*
7. *Worldwide Military Command and Control System (WMCSS).*
8. *Air Force satellite control network.*
9. *Strait of Malacca, the major maritime link between Europe-Arabian Peninsula and the Western Pacific and East Asia.*
10. *National Photographic Interpretation Center (Washington)*

Figure 1: List of Key IW Targets²⁸

inoperable could facilitate strategic and tactical surprise and decrease the warning time available to battlefield commanders by blinding key warning and indication sensors,

disrupting intelligence information analysis systems, and interdicting global communication networks.²⁹

The characteristics of IW practitioners, their motivations, and weapons of attack are just as numerous as the vulnerabilities of information systems and information infrastructure. Different groups, ranging from foreign agents and terrorists to political activists and criminals routinely attack information systems. They attack information systems using a variety of methods including E-mail bombs, logic bombs, ping, computer hijacking, and viruses.³⁰ Generally relying on stealth and persistence to accomplish their task, motivations to attack information systems include greed, espionage, revenge, and curiosity.³¹ Figure 1 provides a notional list of key IW targets.

Summary

In summary, information systems and information infrastructure permeate the entire landscape of everyday society. Information systems currently play an integral role in finance, telecommunications, business, government and the military. Within the US armed forces, information systems directly contribute to a significant increase in lethality of combat forces by facilitating their ability to rapidly process, analyze, and distribute information globally. However, the expansion of civilian and military applications of information systems and its combat multiplying effects on US armed forces are under pressure from IW attackers exploiting systemic vulnerabilities. Open architecture, human factors, and other weaknesses contribute to an environment where IW attackers can easily invade. Utilizing a myriad of sophisticated tools and techniques, the IW attacker undertakes his task to disrupt, destroy, steal and impede information access. The US

armed forces, realizing the threat from IW attack, continue defining doctrine, tactics, and procedures to counter the increasing threat. Analyzing current IW doctrine in response to these attacks illustrates how US armed forces intend to win future IW conflicts.

Effective IW ROE focuses on protecting information, information systems, and information infrastructures. Information represents the “hub of power” US armed forces rely on to command and control forces globally and a key center of gravity which must be protected. Defending the information center of gravity requires IW ROE extend the utmost protection to information systems and information infrastructure. As decisive points in an IW campaign, information systems and infrastructure represent critical nodes effecting both friendly and enemy use of information. To protect information systems and infrastructure, IW ROE should authorize US armed forces to utilize retaliatory and pre-emptive self defense.

Protecting information, information systems, and information infrastructure require maximum protection under IW ROE involves analyzing current US armed forces IW concepts and doctrine and applying joint operational planning doctrine to IW campaigns. Examining IW, in the context of the joint operational planning process, reveals that information systems and infrastructure are critical components of IW ROE design and that future IW campaigns may take on a defensive nature. However, due to various problems associated with implementing purely defensive IW campaigns, the discussion concludes by investigating the shortfalls of centrally controlled defensive forms of IW and the various justifications for utilizing retaliatory and pre-emptive IW attack responses.

Chapter Two: Current State of IW Affairs

Foundational IW Concepts

US armed forces doctrine represents officially sanctioned warfighting principles guiding military actions. Based on experience, history, and the accumulation of knowledge gained through study and analysis, doctrine serves to guide the actions that the US armed forces initiate to support national policy.³² A set of experiences and accumulation of knowledge also serve as the basis for IW. Therefore, subsequent to defining foundational frameworks for IW ROE development, conceptually analyzing IW concepts and doctrine serves to illustrate the path US armed forces currently envision for IW employment.

Because it provides a general framework to formulate military strategy and doctrine, conceptually analyzing IW from an ends, ways, and means approach is a useful tool to understand IW. From military strategy, operational and force developmental strategies, and the doctrine supporting both emerges. An ends, ways and means analysis involves defining objectives or end states, courses of action achieving the objective, and instruments of power that facilitate implementing the selected course of action.³³

IW's objectives or ends represent two ends of a spectrum. On one end of the spectrum, IW's objective is to significantly cripple the capacity of enemy information based militaries to carry out its strategic, operational, and tactical information-dependent processes. The information-dependent processes targeted by IW include command, control, targeting, intelligence, and communication. In achieving this objective, IW denies the enemy effective Command and Control (C²) of his armed forces during conflict.³⁴

Conversely, IW ensures US armed forces information-based processes remain free from interference, interruption, and degradation from opponents. Furthermore, IW also assures US armed forces maintain the unhindered ability to collect, analyze, and distribute information.

To achieve the objective, IW employs various courses of action. A common course of action utilizes IW-Defense or IW-D. IW-D typically involves building a comprehensive network of defenses designed to prevent attack or assure minimum operating levels for critical information infrastructure during and after the attack. Constructing defensive networks generally involves building point and layered defenses around critical information systems and infrastructures. It also typically implements a system providing tactical warning of impending attack, damage control during and after attacks, and repair and restoration of damaged systems.³⁵ An example of layered defenses is the personal computer that employs virus scanning programs, password protection, backup tape or optical drives, and surge protectors to synergistically protect the machine. The virus program works as the tactical warning system by continually scanning for viruses and alerting users to their presence. Passwords provide an additional level of protection by preventing unauthorized access into sensitive areas. Finally, surge protectors serve to maintain service during power fluctuations while backup tape or optical drives provide repair and restoration capability for the system.

While defense is one strategy, offense is another. An offensive strategy controls the information spectrum and prevents adversaries from acquiring, processing, or distributing information. An offensive IW approach involves deterring attack, and failing that, implementing actions to achieve knowledge overmatch. Knowledge overmatch

involves rapidly accessing information to make better informed and faster decisions than an opponent. Achieving knowledge overmatch requires designing simple information access mechanisms, sophisticated methods to retrieve and analyze information, and comprehensive information distribution methods designed to overpower any opponent's ability to match similar capabilities of US armed forces.³⁶ Overmatch also requires a degree of dominance over the electromagnetic spectrum and information infrastructure that ameliorates possible slow downs due to digital friction.³⁷ In this respect, US armed forces typically utilize Command and Control Warfare (C²W) to achieve knowledge overmatch.³⁸

While analyzing IW from an ends, ways and means approach reveals surface relationships, fully understanding IW's dynamics requires closely examining the actual target. Information systems and information infrastructure represent one portion of the IW target set. IW's primary target is the strategic, operational, and tactical command, control, and communications systems making up the command system of the US armed forces. At the core of the US armed forces command, control, and communications processes, lays a command system composed of the organizational structures, standard operating procedures, and technical methods of conveying information that facilitate command and control of tactical combat forces and their ability to direct combat actions achieving mission requirements. The purpose of the command system is to reduce uncertainty in US armed forces decision making processes. It accomplishes this task by using various technical means to collect and process information, analyze the information in accordance with standard operating procedures, and distribute the information throughout the organization.³⁹ Analyzing IW from this perspective reveals that, in its

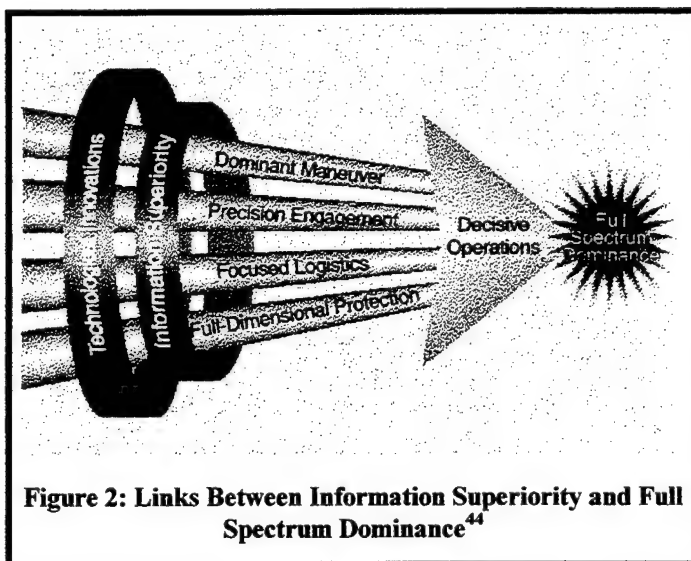
purest form, IW reduces the same uncertainty the adversaries are trying to inject in to US armed forces command systems. Generically, IW reduces uncertainty by preventing opponents from stealing data, disrupting information-based processes, and corrupting or altering information.⁴⁰ Conversely, US armed forces seek to inject uncertainty into adversary command systems by interdicting and disrupting internal information-based processing functions. Accomplishing this task may require US armed forces to steal, disrupt, corrupt, or alter enemy information.

Current IW Doctrine

The US armed forces strategic, operational, and tactical IW doctrine emanates from IW's foundational concepts. The heart of US armed forces IW doctrine is information superiority. Information superiority entails more than merely achieving information parity against adversaries. Rather, information superiority attains a degree of superiority where US armed forces information systems and information infrastructures operate freely and dominate the enemy landscape. For example, achieving information superiority could entail tactical communications systems freely interacting with each other without interference or jamming. Additionally, it could involve strategic decision makers having a clear and uninterrupted continuous information feed on the battlefield situation. In many respects information superiority, outlined in joint doctrine, is analogous to air superiority. Like air superiority, information superiority seeks free exercise of operations without prohibitive interference from adversaries. Like air superiority, information superiority also assumes a degree of freedom to navigate through the GII, NII, and DII while severely limiting an adversary's freedom to utilize the same.⁴¹

Two sources represent IW's tangible implementation in joint doctrine, Joint Publication 3-13.1 Joint Doctrine for Command and Control Warfare, C²W and Joint Vision 2010. C²W combines the disciplines of Electronic Warfare (EW), Psychological Operations (PSYOP), military deception, Operations Security (OPSEC), and physical destruction with intelligence to disrupt, influence and damage enemy information processing capabilities via two methods, C² protect and C² attack.⁴² In joint operations, C²W disrupts the enemy decision cycle while enhancing US armed forces decision cycle by dictating an adversary's operational tempo, disrupting his plans and ability to mass combat power, and influencing his ability to assess the intelligence situation.⁴³ As the doctrinal application of IW, C²W, targets information-based processes, information systems, and information infrastructures and strives for information superiority by assuring friendly dominance of the information spectrum.

Joint Vision 2010, the doctrine and concept for future joint warfighting, also applies and expands IW doctrine. The doctrine for future warfighting rests on the ability of the US armed forces to exploit the information differential and advantages they will



possess by applying advanced technology to strategic, operational, and tactical missions. It's four operational concepts, dominate maneuver, precision engagement, full dimensional protection, and focused logistics,

rely heavily upon IW, information systems and infrastructure to process, analyze, store, protect and disseminate information (see Figure 2). By achieving information superiority, IW creates an environment where Joint Vision 2010 can apply enhanced information technologies and systems that provide comprehensive information access across the breadth and depth of US armed forces operations. Dominate maneuver, the ability to position and effectively employ widely dispersed forces, relies heavily upon IW to ensure information systems and infrastructures maintain the ability to connect and direct dispersed units. Precision engagement, the ability locate and strike targets, and rapidly perform battle damage assessment, relies on information systems to tie together target acquisition, prioritization and tasking mechanisms. Full dimensional protection, the ability to control battle space and ensure freedom of action, rests heavily upon the concept of information superiority. Focused logistics seeks to fuse information with logistics and transportation technology to provide the ability to rapidly ship, track, and deliver vital sustainment. Finally, the combination of all four operational concepts creates a future force dominating the entire spectrum of conflict. At its heart full spectrum dominance relies on IW and information superiority to enhance and protect situational awareness.⁴⁵

IW concepts and doctrine, presents two key issues ROE developers must consider. While IW doctrine rests on achieving information superiority and full spectrum dominance, this does not imply US armed forces can freely employ it without restraint. The potential for collateral damage and unintended consequences of actions taken in cyberspace dictate regulating IW. The interconnection of GII, NII, and DII entails attacks against one will effect the other potentially causing collateral damage. Furthermore, actions taken by US armed forces during times of crises could produce unintended

consequences in an interconnected information infrastructure. For instance, it is relatively unclear whether the US could target hostile forces utilizing the GII located in neutral countries. Military force, whether utilized in retaliation or in pre-emptive fashion, must be proportional in intensity, magnitude, and duration to the situation. Military force, when utilized, must also adhere to internationally accepted laws, treaties, and practices.

On the other end of the spectrum, US armed forces must know the legal, political, moral, and lawful limits within which they can exercise IW. One strength of the US armed forces lies in its ability to freely allow commanders at all levels to exercise judgment, initiative, and expertise to execute the operation that will achieve national objectives. The balance between freely allowing US armed forces' commanders to employ violent and destructive IW versus the necessity to regulate the violence rests in the realm of Rules Of Engagement.

Law of War, ROE & SROE, and Self Defense

Laws of war are the basis for rules of engagement. Within the context of warfare, laws, rules and regulations exist to regulate violence. They exist because of the uncertainty of warfare and because the degradation and chaos that exists on the battlefield and the road of total irrationality down which it can lead combat forces. Laws of war also aim at defining the limits of violence. For the combatants to know who and what they can target, the reason they are targeting them, and the lengths and methods they are allowed to utilize to strike those targets requires carefully defining the limits of violence.⁴⁶

In a modern context, ROE embody laws of war specifying the limits of military action. ROE are “directives issued by competent military authority [which] delineate the

circumstances and limitations which US forces initiate and/or continue the use of deadly (or non-lethal) force.”⁴⁷ They serve to ameliorate the natural tension existing in civil military relations by delineating limits of military action in accomplishment of political objectives. ROE also provide National Command Authority (NCA) guidance to commanders and outline political, legal, and tactical limits for battlefield commanders. They set political constraints on doctrinal principles, tactics, techniques, and procedures.⁴⁸ In a different capacity, ROE serves to manage the tension created by centralized control and decentralized execution. The US armed forces exist in an environment where fielded military forces are distant in both space and time from controlling authorities. The separation coupled with turbulent situations and increased tensions can create an environment where military necessity begins to outweigh the wishes of civilian authorities. Therefore, ROE serves to maintain civilian control of the military at times when tension runs high, soldiers are far from their civilian masters, and the situation is in transition from peace to war.⁴⁹

Implicit in ROE is the inherent right of self defense. ROE emphasize that soldiers, at all levels, possess the inherent right of self defense and nothing shall deny “...a commander’s inherent authority and obligation to use all necessary means available and to take all appropriate action in self-defense of the commander’s unit and other US forces in the vicinity.”⁵⁰ Typically protecting people and organizations, exercising self defense involves utilizing force, proportional in intensity, duration, and magnitude to the situation, when imminent danger exists from hostile acts or hostile intentions.

In October of 1994, the Joint Chiefs of Staff (JCS) published Standing Rules Of Engagement (SROE) defining the inherent right of self defense in two aspects, unit self

defense and national self defense.⁵¹ In terms of unit self defense, SROE further delineated self defense as the act of defending a particular unit of US forces, or an element of it, against hostile act or manifestation of hostile intent.⁵² Implicitly permissive vice directive in nature, SROE primarily encompassed protecting personal, organizations, and "mission essential" equipment from actual or imminent attack. However, with some exceptions, SROE did not clearly address rights of self defense related to protecting military equipment and systems.⁵³

Within the realm of IW, the foundational right of self defense is confusing. Traditional concepts of self defense imply levels of protection with associated mechanisms in place to assure force protection and safeguard human life. However, in most IW scenarios, the target is information systems and infrastructure of a command system. IW seeks to degrade, disrupt, and destroy capabilities and equipment directly associated with decision making while not directly threatening human life. Further adding to the confusion is the issue of "use of force" in retaliation for a violation of rights. Self defense is authorized primarily against deliberate, aggressive, and hostile uses of force violating another nation's sovereignty and rights.⁵⁴ However it remains unclear what targets to attack and the areas to defend in this new networked battlefield. Therefore, the analysis now turns to defining critical IW components, delineating a framework to protect these components, and justifying the application of self defense to protect these components in an offensive manner.

Chapter 3: Foundational IW ROE Concepts

Framework For Protecting IW ROE

Building practical guidelines for IW ROE requires examining the ROE development process. ROE development and review typically takes place during the joint operational planning process and during periodic review of SROE by the Joint Chiefs of Staff.⁵⁵ The joint operational planning process serves as a system to build contingency and operational plans, as the basis for crises action planning, and as a forum to discuss and draft ROE. Joint operational planning builds operational plans to deal with specific military operations. Planners, when devising contingency or operational plans, balance military requirements against various constraints such as strategic mobility, competing military operations, SROE, and legal and political issues. The process of balancing legal and political issues with military requirements gives birth to ROE. Therefore, the joint planning process and ROE development integrally tie together during operational planning.

Examining the pillars of operational plans reveals the basis of ROE development. Planners build operational plans to attack the enemy's key weaknesses while protecting key strengths by identifying and developing plans to exploit enemy vulnerabilities. While multifaceted, this process involves identifying the Center of Gravity (COG), decisive points, and corresponding courses of action to exploit these areas.⁵⁶

A key area of IW operational planning is COG identification. FM 100-5 defines COG as: "the hub of all power and movement upon which everything depends; that characteristic, capability or location from which enemy and friendly forces derive their

freedom of action, physical strength, or the will to fight.”⁵⁷ As an analytical tool, identifying IW COG serves to illustrate the source for friendly and enemy strengths and weaknesses and where the operational plan must mass effects to attain decisive victory while building defenses to prevent defeat.⁵⁸

Because of the critical role it plays within complex military organizations, the IW COG for the US armed forces is information and the assurance of information integrity.⁵⁹ Information serves as the means by which the US armed forces describe and organize themselves. Information and associated control mechanisms also continually bring order to complex and multifaceted combat operations. The increasing complexity of operations, the inability to defeat an enemy with a single blow and the resulting emergence of operational art, demonstrates the necessity to plan and control complex protracted and distributed operations.⁶⁰ Information is central to exercising control over protracted military operations and campaigns. When combined with information systems, information provides feedback on past operations while directing future operations to meet mission outcomes. Information’s key role is to bring order and simplicity to complex military operations. Without information, the ability to control becomes exceedingly difficult.⁶¹

While information is central to controlling complex military operations, other trends also signal the transition of the US armed forces toward information based warfare and the rising importance of information as the COG. Much of the combat power the US military’s conventional forces wield on the battlefield directly relates to the ability to manipulate and control information. The fuel that drives the aspects of warfare which are being computerized, digitized, and automated is information. Furthermore, the ability to

increase lethality of combat forces and while decreasing physical size rests upon information and information access. Finally, the ability to monitor and direct forces globally and its effect in flattening the military organization depends on timely access to information. Conduct of air operations during Desert Storm graphically illustrates the drive toward an information based military. Integration of Joint Surveillance and Target Attack Radar System (J-STARS), Airborne Warning and Control Systems (AWACS) and other sensors enabled airborne control elements to locate time sensitive targets, aerially redirect attack sorties, pass critical target information, and facilitate target destruction.⁶² The future COG for the US armed forces may be information and the ability to access information. Correspondingly, IW ROE development must comprehensively address information and information access issues.⁶³

While planners can identify COG through careful analysis and understanding of the enemy, COG are frequently well protected and difficult to attack. To attack the COG either directly or indirectly requires identifying vulnerable or decisive points. Attacking decisive points produces the greatest destructive effect on the COG. FM 100-5 defines decisive points as "...a point, usually geographical in nature, that, when retained, provides a commander with a marked advantage over his opponent. Decisive points could also include other physical elements such as enemy formations, command posts, and communications nodes."⁶⁴ Decisive points represent keys to attacking the COG and their control allows US armed forces to gain freedom of maneuver.⁶⁵

Identifying decisive point is not a simple task. In order to systematically define decisive points and ensure they ultimately effect the COG requires utilizing a model that defines the enemy information processes and analyzes them for weaknesses. To define

decisive points, John Warden's system of systems approach in combination with detailed "As-Is" model analysis serve as useful tools.⁶⁶ Warden's system of systems analysis involves systematically breaking down five interlocking centers of gravity until the true center of gravity and decisive point emerges.⁶⁷ In his reductionist approach, the five centers of gravity represent a system. Within each system, all five of the centers of gravity reside. Methodically reducing each of these centers of gravity produces the critical or decisive point for the attack or defense. The "As-Is" approach looks at the work flow in progress, identifies how the work is accomplished, and what information systems or infrastructure it relies upon.⁶⁸ Combining both models involves using the "As-Is" approach to outline the macro-level information processes and information centers of gravity within targeted military structures. After identifying macro-level processes, utilizing Warden's system of systems approach classifies and reduces the centers of gravity to decisive points. Comprehensive analysis also requires undertaking this analysis at the strategic operational and tactical levels of warfare.

The analysis of decisive points also needs to address the necessary degree of information integrity required. Defining the necessary degree of information integrity gives planners a range of options to choose from in effecting information decisive points. For example, a key intelligence processing system may require extreme levels of protection to ensure the integrity of system wide data. Conversely, a logistics database may require a lower level of fidelity to ensure parts and equipment are available when required. Analyzing information fidelity defines the point where effective information use stops and information degradation begins. No information system or information infrastructure can ever achieve the desired level of fidelity it's users or producers require.

The very nature of rapidly changing technology and human decision making processes introduces uncertainty into information systems. Whenever incorporating human behavior into an information system, the clash of emotions and independent wills produce an environment where uncertainty exists. Furthermore, military operations in and of themselves reside in chaotic and uncertain environments making the drive for complete precision akin to searching for the "Holy Grail."⁶⁹ Therefore, analysis of decisive points related to information and information systems must address the level of information integrity required.

Information systems and information infrastructure that control both friendly and enemy information flow represent the decisive points US armed force must control to gain information superiority. Information systems and infrastructure represent the control structures necessary for the US armed forces to process, analyze, store, and distribute information. By controlling information systems and infrastructure, US armed forces can dictate information flows to adversaries while assuring continual information flow to friendly forces. In terms of controlling critical systems, examples of decisive points include computer operating systems, network servers, digital data storage facilities, and network communication nodes. Directly or indirectly controlling the information COG requires planners to not only recognize the possibility that information is the COG for US armed forces, but also that information systems and infrastructure represent critical decisive points that must be protected in the information war.

The operational planning process identifies where the enemy derives their strength and defines where US armed forces operations can exert the most influence over that strength. Combining available weapons of warfare, decisive points and specific actions

produces a concrete plan achieving the mission objective of information superiority. This process is called course of action development.

To determine the best way to attack the decisive points requires developing a Course of Action (COA) which will directly or indirectly lead to the decisive point and accomplish mission tasking. COA development serves to combine COG and decisive points with environmental constraints. It produces the most likely COA an IW attacker will utilize to launch IW attack and directs the actions of defenders to counter the attack. One method for developing the most likely enemy and friendly COA is analyzing the information processes of acquisition, processing, distribution, and protection in terms of layered grids of capability. Grids of capability represent the scope, variance, resolution and coverage of any given process. Overlaying each grid produces areas where gaps form and where critical weaknesses develop.⁷⁰ The information acquisition grid represents the availability of all sensors and collectors for a given length of time and the duration, time and frequency of their coverage. The processing grid represents knowledge engines and hardware devices available to process information based on time, capacity, and throughput potential. The distribution grid represents available methods to distribute information throughout a network. Finally, the protection grid represents various defense and attack options available to IW administrators. Overlaying each grid for a given period of time produces a comprehensive look at information system processes and illustrates where potential weaknesses exist.⁷¹

Examining photo intelligence distribution problems during Desert Storm, provides an example where grid analysis could have revealed a critical information system weakness. While air campaign planners had access to current high resolution target

photos at Central Command Headquarters in Riyadh, significant problems developed in the distribution of these photos to Air Force units requiring the information to plan precision guided munition sorties. Due to incompatibilities of the imagery dissemination systems throughout the theater, many pilots briefed and flew with outdated and imprecise imagery. Applying grid analysis could have revealed the shortfall in the photo dissemination system. Overlaying the capabilities of the photo intelligence information system could have revealed that while information acquisition systems were able to acquire the necessary photos, and intelligence analysts were able to process the photo information, the distribution system was unable to pass the information to the tactical units requiring the photos.⁷²

Combining an analysis of COG, decisive points, and COA produces a comprehensive picture of the foundations around which to build a defensive IW operational plan. The general flow of the IW operational plan involves implementing a defensive COA to protect the information center of gravity by controlling the decisive points of information infrastructure and information systems. The defensive COA, which incorporates graduated actions according to varying levels of conflict and threat of attack, seeks information superiority by building defenses around key decisive points in a point and layered fashion. These defenses, which are readily available with current technology, could take the form of enclaves utilizing data replication, separation, and encryption techniques.⁷³ While the ability to track, target and offensively destroy intruders is difficult to implement, judicious use of currently available security measures, close monitoring, and increased security awareness could defeat IW attackers before damage is done. From this

defensive operational plan, IW ROE develops to enhance protection of the information COG, and information systems and infrastructure decisive points.⁷⁴

A defensive IW operational plan and IW ROE supporting it possesses certain inadequacies. A key point is that IW is war. Whether waged on a battlefield or computer terminal, its intent is intervention into the sovereign actions of another denying them the right to make choices and decisions free from coercion. IW's sole purpose is to steal, damage or destroy vital information. Defense by itself is inadequate and its inadequacy dictates that IW ROE preserve the right of combatants at the point of impact to defend either in retaliation to attack or when attack is imminent.

Building a Case for Self Defense: The Inadequacy of Defense Alone

To understand the inadequacy of defense alone, it is useful to revisit the ideas of the Prussian military theorist Carl Von Clausewitz. Clausewitz argued that defense was the stronger form of warfare. He felt defense was stronger because the defender gained an edge with knowledge and selection of terrain to defend, defense's objective sought force preservation, and waiting added relative strength to the weaker defender. Clausewitz balanced defense as the stronger form of warfare with attack as the decisive form of warfare. To Clausewitz, defense had a negative aim, its intent was passive, and it did not increase the ability to wage war or achieve decisive victory. His concept of defense did not passively wait and absorb the attackers blows. The key lay in defending until reaching a critical point where defensive forces could counter attack and achieve victory. In Clausewitz's scenario, the attacker continually lost combat power until reaching a point

where he was no longer able to continue the attack and must defend. Conversely, the defender preserved combat power waiting to go on the offensive.⁷⁵

In a similar fashion, IW defense, by itself is also inadequate. While it is feasible to construct information systems and infrastructure in a way to defend against attack, limits exist to the resiliency of such systems. Waiting and merely enduring each IW attack could eventually lead to a point where US armed forces are no longer able to cope with the attacks, where backup systems become inadequate, and where key information systems and the data they contain extend beyond the point of restoration. In an environment where threats emerge spontaneously and unpredictably, robust information system and infrastructure protection requires a system that anticipates new threats, adapts existing systems, and looks for opportunities to counter-attack IW intruders.⁷⁶

Building a Case for Self Defense: The Inadequacy of Centrally Controlled Attack

While defense alone is inadequate to counter IW attack, centrally controlling counter attack is also inadequate. IW's central characteristics, speed and complexity, continually shrink the dimensions of time and space while simultaneously accelerating the pace of operations.⁷⁷ Today the US armed forces no longer possess the luxury of time to develop and orchestrate war plans which counter electronic attacks occurring within minutes from nebulous threats utilizing a dozen different means.⁷⁸ To counter a distributed threat attacking through multiple means and channels requires a counter attack system designed to execute operations at the point of impact. The historic shift west and subsequent "left hook" ground forces executed during Desert Storm serves as one example of the accelerating pace of operations. The ability to quickly coordinate and

execute the massive move of forces west and the speed at which combat forces gained ground during the conflict required a system where commanders issued orders and where tactical combat units executed the orders based upon judgment and commander's intent. In like manner, it is the increase in velocity of IW and the breadth of the electronic battlefield that prevents a handful of commanders centrally controlling operations. An environment, where a handful of threats utilizing the Internet could attack a dozen sites simultaneously with destructive virus programs, requires US tactical combat forces receive and execute IW operational plans based upon judgment, commander's intent, and analysis of the situation at hand.

The spontaneity and chaos of the information environment coupled with the necessity to possess intelligence at the point of impact also militates against centralized control. The IW environment, its ability to produce new adversaries by the minute, and their ability to attack from hundreds of different sources presents the intelligence community with a challenge to cope with a real time threat. The ability to react "just in time" may be critical to stemming the onslaught of an all out IW attack. In this amorphous and chaotic environment, intelligence must be agile and decentralized to cope with the myriad of potential threats.⁷⁹

While the inadequacies of centralized control dictate a decentralized IW ROE environment where those at the point of attack respond in a pre-emptive or retaliatory fashion, specific problems remain in implementing full autonomy. An environment of decentralized control and execution runs the risk of fratricide and collateral damage. The interconnected nature of the GII, NII, and DII increases the likelihood military units will directly or indirectly target and damage friendly forces on the same network or neutral

forces used as intermediate conduits. To implement fully autonomous operations requires a level of sophistication in information systems, infrastructure and technology necessary to quickly trace and target sources that is currently unavailable.⁸⁰

Summary

Analyzing the joint operational planning process reveals that effective IW ROE must consider how it will protect information and information access. Information is becoming the COG for the US armed forces. It is the “hub of power” from which US armed forces may exert a dominant presence throughout the depth and breadth of the battlefield. To effectively protect information and information access, IW ROE must also carefully ensure it does not compromise protection for information systems and information infrastructure. Controlling both information systems and infrastructure are vital to any IW campaign plan. By controlling information systems and infrastructure decisive points, US armed forces can utilize information to its fullest potential.

While information potentially represents a key COG for the US armed forces and information systems and infrastructures represents the decisive points in an IW campaign, COA analysis reveals that future IW operational plans may rely on defense as the primary means to protect information and information systems. Defensive IW plans may lead planners to draft IW ROE with a defensive bias. However, IW ROE drafters should remember two important points. Building IW ROE based solely on a defensive COA is inadequate unless accompanied by a means to counter attack. IW ROE must preserve the ability for US armed forces to exercise retaliatory and pre-emptive self defense to ensure the counter attack option remains viable. IW ROE drafters must also extend maximum

autonomy to US armed forces who will suffer the brunt of an IW attack. The nature of information warfare, the proliferation of information threats, and the speed and density which attacks may occur dictates a permissive IW ROE environment where forces at the point of impact possess the ability to implement IW counter attack operations with minimal intervention.

Chapter 4: Justifying Self-defense

Legal Justification for Self-defense

In many instances, US armed forces take actions to protect units in self defense largely based on military necessity and mission requirements. However, the justification to exercise pre-emptive or retaliatory self defense relies not only on military necessity but also on a large body of legal, historical, and theoretical precedents. It is also insufficient to justify retaliatory and pre-emptive IW self defense merely because of the inadequacies centralized control or purely defensive forms of IW. Use of force in response to armed attack or threat of armed attack draws its justification from far deeper roots than military necessity. Justifying robust IW ROE authorizing the use of retaliatory and pre-emptive self defense requires examining the legal, historical, and theoretical basis for current self defense concepts.

While the legal water pertaining to IW remains murky and ill-defined, several key legal concepts from the United Nations (UN) Charter and articles justify "use of force," both in a retaliatory and pre-emptive manner. In order to justify use of pre-emptive or retaliatory measures against IW attack, legally it must constitute use of armed attack or act of aggression. An act of aggression, as defined by UN General Assembly Resolution 3314 (1974), is: "...the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."⁸¹ The resolution goes on to specifically state that invasion, attack or bombardment by armed forces of a State, blockade of ports of a State by armed forces, attack by land sea or air forces of

another State, or use of armed forces of one State within another State violating the conditions set forth between the two States constitutes acts of aggression. The resolution does not limit acts of force to this list and may include additional acts as aggression as specified by the Security Council.⁸² UN Charter Article 2(4) lends further clarity to the "use of force" and armed attack concept. Article 2(4) specifically outlaws "...threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations [set forth in Article 1]."⁸³ Finally to clarify the use of force issue, it may be helpful to look at what does not constitute a use of force. Not all violations of international law targeted against another nation constitutes use of force. Economic and political coercion, such as embargoes, under traditional interpretations, does not constitute a use of force.⁸⁴ Therefore, under UN guidelines, IW attacks could be considered acts of aggression and unless authorized by the UN Security Council would constitute an unauthorized armed attack or "use of force."⁸⁵

In response to armed aggression, nations possess the right use force. Article 51 of the UN Charter states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."⁸⁶ Furthermore, the UN Security Council, under articles 39, 41, and 42, authorize use of force pursuant to security council discussion and authorization.

An important point of distinction in Article 51 is the US interpretation. The US argues that Article 51 does not represent an exhaustive list of circumstances authorizing

self defense. Rather it merely codifies a right that has always existed in international law. Furthermore, the US argues Article 51 authorizes exercise of self defense without UN Security Council authorization in cases where it suffers armed attack and in situations other than after actual attack. Under US interpretation, there are two instances where nations can exercise force—in self-defense and when authorized by the UN. In the case of IW, if the act constitutes an act of aggression, the nation suffering the violation is authorized to use force in retribution. However, in all cases of self-defense, the use of force must be necessary and proportional to the act of armed aggression.⁸⁷

While nations may use force under UN auspices, the US uses other legal precedents to justify the use of force in a retaliatory or pre-emptive fashion. They include use of force in peacekeeping and peace enforcement operations, noncombatant evacuation operations, and humanitarian operations.⁸⁸ Furthermore, although not universally accepted, the use of force is also expanding to include rights of self-determination and assistance to those trying to achieve it, and the enlargement of the claims to anticipatory self-defense, responses to terrorism and installing democracies.⁸⁹

Historical Justification for Self-defense

While many legal precedents justify the use of force in self defense, several historic precedents also serve as the traditional basis to justify use of force in cases of imminent danger. One such precedent is the Caroline incident. Known as the Caroline doctrine, the incident and the subsequent rulings and norms it generated served as guidelines for international law for 150 years.⁹⁰ The Caroline incident involved British action taken in 1837 in anticipatory self defense against an insurgency of Canadian rebels. The rebels had

mounted several attacks from islands in the Niagara River. In order to damage the insurgent rebel movement and cut their supply lines, the British attacked the Caroline, a supply ship chartered by the rebels, in US territory. During the attack, the British burned the ship and killed several US citizens. While the US vehemently complained the British had violated the sovereign territory of the US, the British argued they acted in self defense. Analysis of this case established the precedent for use of force in self defense. The conditions authorizing self-defense in a retaliatory and pre-emptive manner were in response to armed attack or imminent threat of armed attack and only in the case where it served as a last resort.⁹¹

While the Caroline incident may serve as historical justification for use of force in self defense, the Corfu Channel case serves to illustrate there is a distinct difference between use of force and armed attack. On 22 Oct 1944, two destroyers from a squadron of British warships suffered damage when they struck mines in the Corfu Channel. After the crippled ships returned to their home port, the British dispatched minesweepers into Albanian waters to sweep the area where the ship's damage occurred. The minesweepers found and disabled a total of twenty mines. After analyzing two of the disabled mines, the British directly attributed the damage to its warships to mines laid in Albanian waters.⁹² In the aftermath of the incident the International Court of Justice ruled that the British had violated Albanian territorial waters but that the act did not constitute armed attack. The Corfu Channel and Nicaragua cases are seen as historical precedents affirming UN Article 2(4).⁹³ Coupling the Corfu Channel case with the UN Charter and Article 2(4), clearly indicates armed attack is use of force but that use of force is not necessarily armed attack.⁹⁴

The distinction between use of force and armed attack is important in defining what actions are considered use of force, what actions are considered armed attack, and what response the recipient can implement. Under Article 51, if a nation suffers armed attack it has the right to respond in self defense. However, as the Corfu Channel case demonstrates, not all uses of force constitute armed attack and thus may not allow the recipient nation to justify response in self defense. The implications for IW ROE from the distinction rests in defining what types of action would be considered armed attack versus use of force. While there is still no authoritative evidence supporting IW attack as armed attack, two circumstances could be used to justify response in self defense to IW attack. One circumstance would be response to "...attacks from directed energy weapons [such as lasers and HERF Guns] and when the consequences are equivalent to the damage done by traditional means."⁹⁵

Theoretical Justification for Self-defense

While historical precedents serve to justify retaliatory and pre-emptive self defense, two theoretical constructs further justify the need to exercise self defensive concepts in response to imminent attack. They include Michael Walzer's criteria for utilizing pre-emptive self defense and the Israeli doctrine of "needle prick." Walzer, a Professor of Social Science at the Institute for Advanced Study in Princeton, New Jersey, argues for legitimate use of first strikes when imminent danger exists from attack. Walzer argues that the instances where nations may legitimately utilize pre-emptive means to prevent attack are when there is sufficient threat from attack. According to Walzer, sufficient threat of attack occurs when there exists "...a manifest intent to injure, a degree of active

preparation that marked that intent a positive danger, and a general situation in which waiting, or doing anything other than fighting, greatly magnifies the risk.”⁹⁶

Under a different justification, the Israeli government asserts the utilization of pre-emptive self defense to prevent a combination of attacks from overwhelming a nation. The Israeli “needle prick” or accumulation of events doctrine asserts that although a single specific act does not constitute a threat in an of itself, a combination of all such incidents may constitute armed attack and entitle the state to pre-emptively attack. Israel argues that unless the nation responds to the lessor acts, it will subject itself to ever increasing levels of violence from which it may not be finally able to respond.⁹⁷

The implications for IW ROE of both Walzer’s theory and the Israeli “needle prick” doctrine clearly demonstrates theoretical justification for pre-emptive attack. In a world where IW attack could occur instantaneously, waiting until the first attack occurs may jeopardize follow-on actions. The loss of one key information infrastructure, such as the regional US air traffic control computer, may not justify armed response. However, the paralyzing effects of system wide attacks against the entire US air traffic control system requires IW ROE strongly consider authorizing pre-emptive self defense.

The IW environment, by its very nature of speed and spontaneity, continually produces warnings and indicators of possible attack. Responding to these indicators requires IW ROE preserve the right to utilize pre-emptive self defense. A modern example of pre-emptive response to hostile IW intent is ROE governing aircraft flying in protection of no fly zones in Iraq. In patrolling skies over Iraq in support of Operations Provide Comfort and Southern Watch, ROE allows aircrew to fire in self defense if threatened by hostile electronic emissions. These emissions generally include, Surface to

Air Missile (SAM) target tracking radars (TTR). ROE authorizes crews to retaliate if threatened with hostile radar emissions. In order for a SAM TTR to lock on and fire at an aircraft, it must first have gone through several steps to acquire, identify and track the aircraft. Once accomplishing these steps, the only step remaining is to illuminate and launch. In some instances, advanced technology SAM systems do not require target acquisition and lock on prior to missile launch. When cockpit indicator's display SAM TTR illumination and launch, it is extremely difficult to determine whether the enemy is spoofing or has launched a missile. With typically only 10-30 seconds from missile launch to impact, crews have little time to request permission to fire. Many times the only recourse an aircraft illuminated by a hostile SAM TTR is to fire pre-emptively.

The response by illuminated aircraft in this example appears to fit all the criteria for actions taken in self defense and may serve as a template for future IW ROE. In the aircraft example, there is an actual or perceived threat that posed imminent danger. The action is hostile and intended to prevent the targeted aircraft from carrying out its mission and performing its duties. Waiting would not only increase the risk but potentially endanger the aircraft and aircrew. No other response is available and firing pre-emptively is proportional to the act of war. In like manner, actual or perceived threats bent on executing hostile actions designed to damage US armed forces information systems and infrastructures permeate the IW environment. Waiting for the attack to occur could increase the risk to entire information system and the only option available to prevent the attack is pre-emptive response.

From the legal, historical and theoretical context, US armed forces possess both the right and obligation to use force in self defense. Furthermore, US armed forces

possess the right to utilize both pre-emptive and retaliatory self defense. IW ROE must be written to allow US armed forces at all levels to exercise this right. IW attack presents a situation where the attack and opportunity to counterattack can occur nearly simultaneously preventing consultation with higher authorities and requiring combatants at the point of attack to respond immediately. Adding intermediate levels of coordination could unnecessarily hinder a tactical commander's ability to respond

Conclusion

Building IW ROE is a process whereby operational level planners take strategic and national guidance and translate them into tactical actions. At the strategic level, IW ROE formulation relies on national policies and guidelines to provide the legal, moral, and ethical boundaries for the US armed forces to employ IW. At the operational level, these policies and guidelines, along with operational requirements, are translated into operational plans and ROE. At the tactical level, operational plans are executed within the confines of the legal, moral, and ethical limits placed on them by the NCA.

While nationally there is a realization that information is critical to the survival of the US, the country lacks a comprehensive national information policy addressing vast information concerns. Both the National Security Strategy and National Military Strategy state information infrastructure and information superiority are keys to many national functions. However, both documents do not address the information strategies and policies of the US government.⁹⁸ The US lacks a comprehensive document outlining policies an information based society will use to form its values, international interactions, and behaviors. A national information policy outlines how the US will deal with actors and agents in a networked world. It also announces US policies should threats to our national information interests arise. Finally, a national information policy "...delineates intangible values, ethical positions, national security and the thresholds over which another nation-state must not cross" and how the US will deal with a myriad of issues emerging in the transition to and information-based society.⁹⁹

Strategically building effective IW ROE with robust self defense mechanisms requires a comprehensive US information policy. IW ROE also requires an organization within the Department of Defense (DoD) which specifically addresses the unique concerns of the US armed forces.¹⁰⁰ Currently many organizations, such as the Director of Central Intelligence, the Defense Intelligence Agency, the Joint Staff, individual military departments, and combatant commands, play a role in IW. However, there is not a single focal point within the DoD controlling IW affairs. IW's interdisciplinary nature requires the Secretary of Defense designate a single focal point to deal with the vast IW concerns of the US armed forces. This focal point for IW, the Assistant Secretary of Defense for IW (ASD-IW) would serve several functions. The ASD-IW would serve as the primary agency providing staff supervision for all information warfare related issues. Building upon the national information policy, the ASD-IW could also outline the US armed forces military information policy. This military information strategy would serve as the cornerstone for IW operational planning and ROE development. Specifically, the military information strategy would outline critical information resources and systems. The military information strategy could also delineate the jurisdictional responsibilities for protecting key information systems and infrastructure and the limits within which these protections can be extended. Finally, the ASD-IW focal point could outline the tactical limits of retaliatory and pre-emptive self defensive actions US armed forces could execute in event of attack.

A clearly defined national and military information strategy and a central DoD IW focal point empowers operational planners to design operational plans and IW ROE supporting national security interests and countering global threats. While IW ROE

development eventually depends upon strategic development of national information policy, practical experience and systematic implementation of IW concepts throughout the US armed forces also forms the basis for IW ROE. Although efforts are underway toward implementing IW plans, comprehensive implementation within the US armed forces remains in the prodromal stages. IW ROE will gain further definition as structural changes occur, doctrine develops and matures, and efforts increase to research and develop new techniques to wage IW.

As the discipline of IW continues maturing and operational planners experiment with various techniques to implement offensive and defensive IW, the structure of the US armed forces may change to incorporate new organizations. Changes at the tactical level of combat may cause revisions to existing national and military information policies. The US Air Force's 609th Information Warfare Squadron (IWS) is one example where tactical application may change the landscape of IW ROE. The 609th IWS, located at Shaw AFB, South Carolina, is the Air Force's first attempt to develop an entire organization dedicated to conducting defensive IW.¹⁰¹ While the current mission is defensive, the 609th IWS, in conjunction with other efforts throughout the Air Force may be researching technological and doctrinal techniques to implement offensive actions. The emergence of new offensive techniques may force IW ROE drafters to carefully consider the impact of automated attack response systems, electronic precision attack systems, and isolation routines on international agreements.¹⁰² As tactical application of offensive IW becomes widespread throughout the US armed forces, IW ROE drafters may encounter situations requiring close examination of legal and moral ramifications IW actions. Questions will certainly

arise as to the legal and procedural issues governing the potential use of a tool affecting many people in a networked environment.

Comprehensive implementation of IW and the corresponding development of IW ROE will also raise other areas which must be debated and addressed. One issue is how IW ROE will regulate the area of offensive IW. Issues, such as legal access, free speech, and national sovereignty, emerge from applying the principles of the conventional battlefield to cyber-battlefield. An additional concern is targeting and collateral damage. Launching offensive strikes over a network may inherently effect innocent bystanders. Furthermore, the second and third order effects of damaging key information infrastructure may drastically alter the internal landscape of the enemy.¹⁰³ Ethical dilemmas may also arise in the area of the interworking of military ROE and civilian domestic law. Issues concerning free speech and universal access to information balanced against the necessity to protect key military information and infrastructures will continue to emerge as IW ROE matures. Questions concerning the role the military should play in domestic IW operations may also spur key legal and political debates in the future.

The issues which will shape the future debate over IW ROE should not detract from the central focus of IW. For IW ROE to be effective it should carefully consider how it will protect information. As a potential COG for the US armed forces, information, information superiority, and information access is becoming increasingly essential to planning and implementing future combat operations and future joint doctrine. To protect information, IW ROE should carefully consider how it will extend protection to key information systems and infrastructure. Information systems and infrastructure are decisive points which influence how the US armed forces process, analyze, and distribute

information. Finally, effective IW ROE should extend the right of US armed forces to use retaliatory or pre-emptive self defense. Extending the right to respond in self defense ensures information systems and infrastructure will remain viable in an environment where threats emerge spontaneously and without warning.

Endnotes

¹ Bradd C. Hayes, *Naval Rules of Engagement: Management Tools for Crisis* (Santa Monica: Rand, 1989), p. 2

² For a complete analysis of the complexities of just and unjust wars refer to Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, (New York: Harper Collins, 1992)

³ Martin van Creveld, *The Transformation of War*, (New York: The Free Press, 1991) p. 89

⁴ *New York Times* book reviewer Jed Harris calls "The Cuckoo's Egg" both "a gripping spy thriller and an intriguing introduction to the futuristic world of international computer networking." Jed Harris, review of *The Cuckoo's Egg* by Clifford Stoll *New York Times*, 26 November 1989, p. L-7

⁵ Stoll named the program a cuckoo's egg after the cuckoo bird. Cuckoo birds lay their eggs in other birds' nest. The cuckoo chicks survival rests on the ignorance of the hen hatching the egg. In this instance the "cuckoo's egg" program was designed to hatch and feed the intruder superuser privileges similar to Stoll's to ensure continued undetected access to the Lawrence Berkeley system. Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, (New York: Doubleday, 1989) p. 23

⁶ Tynmet was a precursor to the Internet which interconnected the computers and computing centers of many universities, and government agencies around the nation. Stoll, p. 207

⁷ Stoll nicknamed the sting "Operation Showerhead" because the uncanny timing of the hackers activities seemed to coincide with every time he was in the shower. Stoll, p.207

⁸ Stoll, pp. 275-279

⁹ David A. Fulghum, "Computer Combat Rules Frustrate the Pentagon," *Aviation Week and Space Technology*, Sept 15, 1997, p. 67

¹⁰ Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994) p. 49

¹¹ Office of the Joint Chiefs of Staff Joint Electronic Library, *Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W)*, Washington DC: U.S. Government Printing Office 1996, p. I-3; Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age*, (Fairfax: AFCEA International Press, 1996) pp. 10, 23-26, 43, 165; Office of the Secretary of

Defense, Information Warfare - Defense, Washington DC: U.S. Government Printing Office, 1996, pp. ES-3, 2-4, H-4

¹² Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), Washington DC: U.S. Government Printing Office 1996, p. I-1 & 2; Thomas G. Mahnken, "War in the Information Age", *Joint Force Quarterly*, Winter 1995-96, p. 40; Office of the Joint Chiefs of Staff Joint Electronic Library, Concept for Future Joint Operation, Expanding Joint Vision 2010, Washington DC: U.S. Government Printing Office, May 1997, p. 39

¹³ Campden, p. 20 & 92; Schwartau, p. 54; Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), p. I-2 & 3; Concept for Future Joint Operation, Expanding Joint Vision 2010, p. 84

¹⁴ Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010, Washington DC: U.S. Government Printing Office, p. 16; Tom Barrows, "Information Operations," *A Common Perspective*, March 1997, vol. 5 no.1, p. 13

¹⁵ Schwartau, p. 52;

¹⁶ Charles Swett, "Strategic Assessment of the Internet", Office of the Secretary of Defense for Special Operations and Low-Intensity Conflict, 17 July 1995.

¹⁷ Schwartau, p. 52

¹⁸ Campden, p. 19

¹⁹ *Wall Street Journal* (New York) 24 October 1997

²⁰ The Commission's (PCCIP) basic mission is to advise and assist the President by recommending a national strategy for protecting and assuring critical infrastructures. To do this, the Commission identifies and categorizes threats (physical or cyber), considers vulnerabilities, and develops policy and legislative options necessary to effect the recommendations and implement the plan. PCCIP was chartered under Presidential Executive Order 13010 in July of 1996. Its chair is Robert "Tom" Marsh and includes senior representatives from private industry, government and academia. In addition to its civilian membership, PCCIP is comprised of two members from Department of Treasury, Justice, Defense, Commerce, Transportation, and Energy. Additional participating executive branch members of the group include Central Intelligence Agency, Federal Emergency Management Agency, Federal Bureau of Investigation, and The National Security Agency. "President's Commission on Critical Infrastructure Protection," [Document on-line] (Washington DC: The White House, 1996, accessed on 26 Oct 1997); available from <http://www.info-sec.com/pccip/web/>; Internet

²¹ Jack L. Brock, "GAO Executive Report B-266140." [Document on-line] Washington DC: accessed Oct 1996); available from http://www.infowar.com/civil_de/gaosum.html; Internet

²² For an overview of these systems refer to Office of the Joint Chiefs of Staff Joint Electronic Library, "Joint Doctrine Encyclopedia (Draft)." Washington DC: U.S. Government Printing Office; For an overview of the information systems and information infrastructure contained within GCCS refer to Office of the Joint Chiefs of Staff Joint Electronic Library, CJCSM 3500.03 Joint Training Manual for the Armed Forces of the United States. Washington DC: U.S. Government Printing Office, p. annex A to Appendix L.

²³ For additional information on civilian related computer attacks refer to Scott Charney, "Computer Crime" Department of Justice, Criminal Division, 1996, p. 6; George I. Seffers, "U.S. Readies Vaccine To Fight Virtual Virus," *Defense News*, (September 22-28, 1997) p. 1 & 60; "Information Warfare-Defense", p. 2-15; Brock, p. 4

²⁴ Brock, pp. 13-14

²⁵ Ibid., pp. 14-16

²⁶ A "back door" is a file inserted into a computers operating system designed to circumvent existing security measures.

²⁷ Systems designed with open architecture seek to make access from public networks and network services from any number of network and non-network related service providers readily available, "Information Warfare-Defense," p. 2-10

²⁸ Arsenio T. Gumahad, "The Profession of Arms in the Information Age," *Joint Force Quarterly*, Spring 97, p.18

²⁹ Mark R. Jacobson, "Justifying Self-Defense in the Age of Non-Armed Attack," Columbus: The Ohio State University, 1996, p. 11

³⁰ E-mail bombing involves sending millions of E-mail messages intent on overloading phone services and crashing networks. Logic bombs are programs activated by key words or phrases with the intent of causing harm to computer systems. An example of a logic bomb would be the activation of a program designed to erase a computer hard drive when the user types in the phrase "Mickey mouse." Pinging involves deliberately sending a ping or packet of data larger than 65,536 bytes to a remote machine. Depending upon the computers operation system, the result of pinging could be to crash, reboot, or kill a significant number of systems. Computer hijacking involves intruders stealing passwords and taking over systems such as air traffic control. Viruses are segments of software written to implant themselves into key operating system files and adversely affect the host

computers operation. They are typically designed to infect system unknowingly and can be either benign or malignant. "Presidents Commission on Critical Infrastructure Protection"; Schwartau, p. 104; "Symantec Antivirus Research Center."

³¹ "Information Warfare-Defense," p. 2-13; "Symantec Antivirus Research Center"; Schwartau, pp. 87-93;

³² U.S. Air Force, Air Force Manual 1-1, Basic Aerospace Doctrine of the United States Air Force, Washington DC: U.S. Government Printing Officer, 1997, p. 1

³³ Arthur K. Lykke, "Toward an Understanding of Military Strategy," Command and General Staff College, Ft Leavenworth, KS, 12 March 1993

³⁴ Blake Harris, "Advent of Information Warfare," [Internet Document] <http://www.i-war.com/advent.htm>, p. 1-3; Office of the Secretary of Defense, "Information Warfare - Defense," p. 2-1

³⁵ "Information Warfare - Defense," p. ES-2 to ES-4.

³⁶ A key component of knowledge overmatch is the knowledge engine. A knowledge engine is a sophisticated information retrieval architecture designed to mine information sources, extract pertinent data, divide and analyze the data, form models from the data to predict future events, and allow the user to evaluate the model to find critical vulnerabilities. In this aspect, the knowledge engine is similar to the intelligence officer who spends years of training and study to build threat models and predict enemy courses of action. It is this new and developing critical capability which must be protected. Schneider, Michael W., Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel? SAMS Monograph, Fort Leavenworth, 1994, pp. 10-22

³⁷ Digital friction involves the physical and electronic limits over which new technology or innovations in science must be utilized to achieve a new level of performance. An example of digital friction is radio range or line of sight constraints. Schneider, p. 10, 36-40

³⁸ Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), p. I-4

³⁹ Martin van Crevald, Command in War, (Cambridge: Harvard University Press, 1985) pp. 261-269

⁴⁰ Campen, p. 93

⁴¹ U.S. Air Force, Air Force Manual 1-1, Basic Aerospace Doctrine of the United States Air Force, Washington DC: U.S. Government Printing Officer, 1992, p. 273

⁴² C2 protect involves “maintaining effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.” C2 attack “Prevents effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.” Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), pp. I-4

⁴³ Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W), pp.I-1 to I-7

⁴⁴ Concept for Future Joint Operation, Expanding Joint Vision 2010, p. 58

⁴⁵ Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 1.0 Joint Doctrine of the Armed Forces of the United States, Washington DC: U.S. Government Printing Office 1996, p. IV-9; Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010. Washington DC: U.S. Government Printing Office, pp. 16 & 19-27; Concept for Future Joint Operation, Expanding Joint Vision 2010, p. 24; “Information Warfare - Defense,” p. 2-1

⁴⁶ van Crevald, Martin. The Transformation of War, pp. 87-94

⁴⁷ Office of the Joint Chiefs of Staff Joint Electronic Library, JTF Commanders Handbook For Peace Operations, Washington DC: US Government Printing Office 1996, p. 74

⁴⁸ James J. Tritten, “Naval Perspective for Military Doctrine Development,” Joint Electronic Library, Washington DC: US Government Printing Officer, 1996, p. 13

⁴⁹ Hayes, p. 2

⁵⁰ Enclosure A, *Standing Rules of Engagement For US FORCES* [Internet Document: www.eucom.smil.mil/eccs-as/library/documents/roe.ea.html], 1997

⁵¹ JTF Commander’s Handbook for Peace Operations, pp. 73-78

⁵² Hayes, p. 77

⁵³ Office of the Joint Chiefs of Staff, Standing Rules of Engagement, Washington DC: U.S. Government Printing Office, 1993

⁵⁴ “A Primer on Legal Issues in Information Warfare,” p.11, Author unknown

⁵⁵ SROE are periodically reviewed by the Secretary of Defense and the Joint Chiefs of Staff to ensure conformity of SROE and ROE issued by unified and specified commanders. For a complete overview of the joint operational planning process refer to

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3.0 Doctrine for Joint Operations, Washington DC: U.S. Government Printing Office 1996; Hayes, p. 33-34

⁵⁶ While COG, decisive points and courses of action are critical parts of the operational planning process, it is their link to the mission requirements, tasks and objectives that drives the beginning of the process. Many of the operational plans are initiated from a series of documents and strategies. The National Security Strategy and National Military Strategy along with the Joint Strategic Capabilities Plan (JSCP) formulate the requirement for operational planning.

⁵⁷ U.S. Army, FM 100-5 Operations, Washington DC: U.S. Government Printing Office, 1993, Glossary 1

⁵⁸ Joint Pub 3.0 Doctrine for Joint Operations, pp. III-20 and III-21

⁵⁹ Campden, pp. 197-198

⁶⁰ For a complete description of operational art and its emergence see Schneider, James J., "The Theory of Operational Art", Theoretical Paper No. 3, School of Advanced Military Studies, Ft Leavenworth, 1 March 1988.

⁶¹ James J. Schnieder, *Black Lights: Chaos, Complexity, and the Promise of Information Warfare. Joint Force Quarterly* (Spring 97) pp. 27

⁶² During Operation Desert Storm the continuous coverage of air breathing and space based reconnaissance and attack platforms, aimed at finding and destroying SCUD missiles, represent the flexibility and vitality information and information systems provided. Continuous airborne surveillance coupled with attack aircraft, either airborne or on alert, were employed to track, target and destroy individual missile launchers. For a further explanation see Thomas A. Keaney and Eliot A. Cohen, Gulf War Air Power Survey Summary Report, (Washington DC: Library of Congress, 1993) p. 17

⁶³ Alvin Toffler and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. (Boston: Little, Brown, and Company, 1993) pp. 69-79

⁶⁴ FM 100-5 Operations, p. Glossary-2

⁶⁵ Joint Pub 3.0 Doctrine for Joint Operations, pp. III-21 & III-22

⁶⁶ Col John Warden, USAF (ret.), is a modern day air power theorist and originator of many of the strategic concepts surrounding the air campaign undertaken during Desert Storm. His writing includes "The Air Campaign" and many companion articles. Studying Warden's system of systems approach reveals many of the theoretical underpinnings of current Air Force doctrine and serves as a useful tool to manipulate and apply in concert

with “As-Is” model analysis. While analyzing Air Force doctrine may demonstrate application of his theory’s, some of Warden’s theoretical constructs useful to this discussion were altered or omitted from current air force doctrine.

⁶⁷ Warden’s five centers of gravity include leadership, organic essentials, infrastructure, population and fielded forces. The centers of gravity are arranged concentrically with leadership residing in the inner ring and fielded forces residing on the outer ring. Under Warden’s concept, leadership represents the most important of all the rings and should be the focus of military campaigns. For a complete synopsis of Warden’s concepts see Phillip S. Meilinger, The Paths of Heaven: The Evolution of Airpower Theory, (Maxwell Air Force Base, Montgomery Alabama: Air University Press, 1997) pp. 371-384

⁶⁸ The “As-Is” model is similar to business process reengineering. It typically asks three questions when analyzing a system that must be changed, developed or updated. These questions are: “What is being done (business model)? How and when is it done (work and information models)? What computing and communications infrastructure and supporting facilities does the function(s) depend upon (technical model)? While the model is relatively easy to apply in a business environment, its application against an enemy force is complicated by inability to gain intelligence access to many human related processes. Campden, pp. 166-167

⁶⁹ Van Crevald, Martin, Command in War, pp. 264-268; Campden, p. 171; Mahnken, p. 42

⁷⁰ Campden, p. 199-201

⁷¹ The process of grid analysis is similar to land operations and the construction of the Modified Combined Obstacle Overlay (MCOO) The MCOO analyzes key terrain and most likely avenues of approach enemy or friendly forces could utilize to execute operations. The MCOO, combined with doctrinal templates, serves to produce possible enemy COAs.

⁷² Keaney, pp. 134-137

⁷³ IW enclave defense involves building information systems and infrastructure safe zones protected by barriers and which is continually monitored, controlled and defended. Within the enclave, an environment, free from outside threat, is established where users can roam freely. Any outside contact is carefully screened ensuring threats do not enter the system. Enclaves are typically built using firewalls or electronic barriers preventing outside attack and isolating the system. Data replication involves techniques designed to copy and store critical data. Campden, pp. 168-172

⁷⁴ Schwartau, pp. 312-315; Campden, pp. 91-105, 169-172

⁷⁵ Carl von Clausewitz, On War. Princeton: Princeton University Press, 1976, pp. 357-392

⁷⁶ Campden, p. 80

⁷⁷ Toffler, p. 141-142, Campden, pp. 170, 201

⁷⁸ Campden, p. 80

⁷⁹ Ibid., p. 79-80

⁸⁰ To solve the problem of identifying the location of users on the Internet, one theory holds that electronic signatures using GPS could be attached to everyone logging into the system. Interrogating these signatures would allow those tracking and tracing intruders quicker and easier access. See Campden, pp. 119-126

⁸¹ "Information Warfare and the Use of Force Among Nations," p. 2

⁸² Ibid., pp. 2-3

⁸³ Jacobson, p. 14

⁸⁴ James N. Bond, "Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)," Office of the Secretary of Defense, pp. 54-55

⁸⁵ Electronic Mail to Ted Uchida from CDR James N. Bond, Response to questions concerning the legal ramifications of the inherent right of self defense in IW, 21 July 1997

⁸⁶ "Information Warfare and the Use of Force Among Nations," p. 6

⁸⁷ Electronic Mail to Ted Uchida from CDR James N. Bond, Response to questions concerning the legal ramifications of the inherent right of self defense in IW, 21 July 1997

⁸⁸ A Primer on Legal Issues in Information Warfare, p. 11

⁸⁹ Bond, "Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)," p. 63

⁹⁰ Alexander Deconde, A History of American Foreign Policy, Volume I: Growth to World Power (1700-1914), (New York: Charles Scribner's Sons, 1978, pp. 140-142,149); Jacobson, p. 16

⁹¹ Jacobson, p. 15-16

⁹² "The Corfu Channel Case (Great Britain-Albania)" [Document on-line] (accessed on 26 Oct 1997); available from <http://www.trincoll.edu/~pols/Courses/POLS312/SOVcases.HTML#THE CORFU>, pp. 2-4

⁹³ The Nicaragua case involved the International Court of Justice decision pertaining to cross border incursions by Nicaraguan military forces into Honduras and Costa Rica. The court held that Nicaraguan provision of arms to El Salvadorian rebels did not constitute armed attack, Bond, p. 56-57

⁹⁴ Ibid., p. 56

⁹⁵ Information Warfare and the Use of Force Among Nations, p. 5-6

⁹⁶ Walzer, p. 81

⁹⁷ Jacobson, "Justifying Self-Defense in the Age of "Non-Armed Attack," p. 22

⁹⁸ National Security Strategy and National Military Strategy outline broad guidelines and national interests for the US. Formed as the result of the Goldwater-Nichols Defense Reorganization Act, they serve to outline US vital national interests and how the US armed forces will safeguard those interests.

⁹⁹ Campden., p 248; A national information policy will serve to address many different issues. It will seek to define information as a overriding security interest and the measures the US will take to protect this vital national interest. It will seek to define what is information, how it is represented and where it value is derived. It will also seek to quantify the importance of information, establish ownership criteria and rule governing its dissemination. A national information policy will seek to define international boundaries within a globally networked world as well as establish jurisdictional boundaries between federal and state authorities. Schwartz, pp. 316-342

¹⁰⁰ "Information Warfare - Defense," p. 6-1

¹⁰¹ O'Malley, Chris, Information Warriors of the 609th. (Air Force's 609th Information Warfare Squadron), [Internet Document] (Popular Science, vol. 251, No.1, accessed on 31 Oct 1997), available from [http:// www.infowar.com/mil_c4i/mil_c4i_100397a.html-ssi](http://www.infowar.com/mil_c4i/mil_c4i_100397a.html-ssi), pp. 1-5

¹⁰² An isolation routine is a set of software instructions designed to isolate a given information system from its outside links. The routine can be likened to building walls around a system not permitting it to interact with outside environments. This concept can be further extended to nations. Isolation routines could be enabled preventing nations from utilizing many of the electronic media from interacting on the GII. Campden, p, 243-248

¹⁰³ The problem of collateral damage as an issue for IW falls in the arena of attacks on infrastructure of another nation. While the attacks themselves do not directly kill people, the second and third order effects of destroying the information infrastructure controlling water treatment and electrical generation and distribution could be devastating in the long term.

Bibliography

Books

Allard C. Kenneth. Command, Control, and the Common Defense. New Haven: Yale University Press, 1990.

Brinton, Crane. The Anatomy of Revolution. New York: Random House, 1965.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden. Cyberwar: Security, Strategy, and Conflict in the Information Age. Fairfax: AFCEA International Press, 1996.

Clausewitz, Carl Von, On War. Princeton: Princeton University Press, 1976.

Corbett, Julian. Some Principles Of Maritime Strategy. Annapolis: Naval Institute Press, 1988.

Deconde, Alexander, A History of American Foreign Policy, Volume I: Growth to World Power (1700-1914). New York: Charles Scribner's Sons, 1978.

De Landa, Manuel. War in the age of Intelligent Machines. New York: Zone Books, 1991.

Hayes, Bradd C., Naval Rules of Engagement: Management Tools for Crisis. Santa Monica: Rand, 1989.

Keaney, Thomas A. and Eliot A. Cohen, Gulf War Air Power Survey Summary Report. Washington DC: Library of Congress, 1993.

Meilinger Phillip S., The Paths of Heaven: The Evolution of Airpower Theory. Maxwell Air Force Base, Montgomery Alabama: Air University Press, 1997.

The Merriam Webster Dictionary. Springfield: Merriam Webster, 1994.

Quittner, Joshua and Michele Slatalla. Masters of Deception, the Gang that Ruled Cyberspace. New York: Harper Collins, 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Snyder, Frank M. Command and Control: The Literature and Commentaries. Cambridge: Harvard University, 1989.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday, 1989.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown, and Company, 1993.

van Crevald, Martin. The transformation of War. New York: The Free Press, 1991.

_____. Command in War. Cambridge: Harvard University Press, 1985.

Waldrop, W. Mitchell, Complexity, The Emerging Science At The Edge of Order and Chaos. New York: Touchstone Book, 1992.

Walzer, Michael, Just and Unjust Wars: A Moral Argument with Historical Illustrations. New York: Harper Collins, 1992.

Warden, John A. III, The Air Campaign: Winning for Combat. Washington DC: NDU Press, 1988.

Articles

Barrows, Tom, "Information Operations." A Common Perspective, (March 1997, vol 5 no.1).

Boorda, Jeremy M., "Leading the Revolution in C4I." Joint Force Quarterly (Autumn 1995)

Burton, Daniel F., "The Brave New Wired World." Foreign Policy (Spring 1997) pp. 23-38

Fulghum, David A., "Computer Combat Rules Frustrate the Pentagon." Aviation Week and Space Technology (Sept 15, 1997)

Gumahad, Arsenio T., "The Profession of Arms in the Information Age." Joint Force Quarterly, (Spring 97) p.19

Harris, Jed, "Nabbed on the Data Highway." New York Times (26 November 1989) p. L-7

Humphries, John G., "Operations Law and the Rules Of Engagement In Operations Desert Shield and Desert Storm." Airpower Journal (Fall 1992) pp. 25-41.

Kraus, George F. "Information Warfare in 2015." U.S. Naval Institute Proceedings (August 1995), pp. 42-45

Mahnken, Thomas G., "War in the Information Age." Joint Force Quarterly (Winter 1995-96) p. 42

Mathews, Jessica T., "Power Shift." Foreign Affairs (January/February, 1997) pp. 50-66

Nye, Joseph, William Owens, and Eliot Cohen. "The Information Edge." Foreign Affairs (March/April 1996) pp. 20-36

Rosecrance, Richard. "The Rise of the Virtual State." Foreign Affairs (July/August 1996) pp. 45-61

Ryan, Donald E., "Implications of Information-Based Warfare." Joint Force Quarterly (Autumn-Winter 94-95) pp. 114-116.

Schnieder, James, J., "Black Lights: Chaos, Complexity, and the Promise of Information Warfare." Joint Force Quarterly (Spring 97) pp. 21-28

_____, "The Theory of Operational Art", Theoretical Paper No. 3, School of Advanced Military Studies, Ft Leavenworth, 1 March 1988. pp. 1-53

Seffers, George I., "U.S. Readies Vaccine To Fight Virtual Virus." Defense News. (September 22-28, 1997) pp. 1 & 60

Struble, Dan. "What is command and control warfare?" Naval War College Review, (Summer 95) pp. 89-98.

Tritten, James J., "Naval Perspective for Military Doctrine Development." Joint Electronic Library, Washington DC: US Government Printing Office, 1996

Vincent, Gary A., "In the Loop, Superiority in Command and Control." Airpower Journal (Fall 1992) pp. 15-25.

Government Documents

Office of the Joint Chiefs of Staff Joint Electronic Library, CJCSM 3500.03 Joint Training Manual for the Armed Forces of the United States. Washington DC: U.S. Government Printing Office, May 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Concept for Future Joint Operation Expanding Joint Vision 2010. Washington DC: U.S. Government Printing Office, May 1997.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Doctrine Encyclopedia (Draft). Washington DC: U.S. Government Printing Office, May 1997.

Office of the Joint Chiefs of Staff, JCS Memo of Policy (MOP) 30, Command and Control Warfare. Washington DC: U.S. Government Printing Office, 1993.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Vision 2010. Washington DC: U.S. Government Printing Office, May 1997.

Office of the Joint Chiefs of Staff Joint Electronic Library, JTF Commander's Handbook for Peace Operations. Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 1.0 Joint Doctrine for Command and Control Warfare (C2W). Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3.0 Doctrine for Joint Operations. Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff Joint Electronic Library, Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W). Washington DC: U.S. Government Printing Office, 1996.

Office of the Secretary of Defense, Information Warfare - Defense. Washington DC: U.S. Government Printing Office, 1996.

Office of the Joint Chiefs of Staff, Standing Rules of Engagement. Washington DC: U.S. Government Printing Office, 1993.

Science Applications International Corporation. Planning Considerations for Defensive Information Warfare - Information Assurance. Washington DC, 1993.

U.S. Air Force, Air Force Manual 1-1, Basic Aerospace Doctrine of the United States Air Force. Washington DC: U.S. Government Printing Office, 1992.

U.S. Army, FM 100-5 Operations. Washington DC: U.S. Government Printing Office, 1993.

U.S. Army, FM 27-10, The Law of Land Warfare. Washington DC: U.S. Government Printing Office, 1956.

Army War College

Metz, Steven, Strategic Horizons: The Military Implications of Alternative Futures. U.S. Army War College, Carlisle Barracks, 1997.

School of Advanced Military Studies

Schneider, Michael W., Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel? SAMS Monograph, Fort Leavenworth, 1994.

Smith, Kevin B., The Crises and Opportunity of Information War. SAMS Monograph, Fort Leavenworth, 1994.

Theses, Studies, and Other Papers

A Primer on Legal Issues in Information Warfare. No author and no date published apparently written as a point paper for briefing to USAF Air Staff.

Bond, James N., Peacetime Foreign Data Manipulation As One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4). 1996.

Burton, Michael A., Rules of Engagement: What is the Relationship Between Rules of Engagement and the Design of Operations? SAMS Monograph, Fort Leavenworth, 1987.

Charney, Scott. Computer Crime. Department of Justice, Criminal Division, 1996.

Grotzky, Craig L. The Impact of the Standing Rules of Engagement (SROE) On Peace Enforcement Operations. Naval War College (Newport, 12 February 1996).

Information Warfare and the Use of Force Among Nations. No author and no date apparently written as background information for ROE development officials on USAF Staff.

Jacobson, Mark R. Justifying Self-Defense in the Age of "Non-Armed Attack." Columbus: The Ohio State University, 1996

Krepinevich, Andrew F., Keeping Pace with the Military-Technological Revolution. Military Technology, 1994.

E-Mail and Other Electronic Documents

Brock, Jack L., "GAO Executive Report B-266140." [Document on-line] Washington DC: accessed Oct 1996); available from http://www.infowar.com/civil_de/gaosum.html-ssi; Internet

CDR James N. Bond response to questions concerning the legal ramifications of the inherent right of self defense in IW. 1 July 1997-30 August 1997

Mark Jacobson response to questions concerning the implications of exerting the inherent right of self defense in IW. 1 July 1997-30 August 1997

Dr. Dan Kuehl response to question concerning the inherent right of self defense and it's relationship to IW. 1 July 1997-30 August 1997

O'Malley, Chris, "Information Warriors of the 609th. (Air Force's 609th Information Warfare Squadron)." [Internet Document] (Popular Science, vol. 251, No.1, accessed on 31 Oct 1997), available from http://www.infowar.com/mil_c4i/mil_c4i_100397a.html-ssi

"The Corfu Channel Case (Great Britain-Albania)" [Document on-line] (accessed on 26 Oct 1997); available from <http://www.trincoll.edu/~pols/Courses/POLS312/SOVcases.HTML#THE CORFU>.

"President's Commission on Critical Infrastructure Protection," [Document on-line] (Washington DC: The White House, 1996, accessed on 26 Oct 1997); available from <http://www.infosec.com/pccip/web>; Internet.

"Symantec Antivirus Research Center," [Document on-line] (Symantec Corporation, 1996/1997, accessed on 26 Oct 1997); available from <http://www.symantec.com/avcenter/vinfodb.html>; Internet.